# Technical Cybersecurity

Binutils

# Extending your Lab

## Currently Penetration Oriented

- Networked, scannable, vulnerable hosts

## Adding binary analysis capabilities

- We’re going to create a new workstation
- Ubuntu LTS
- Binary analysis tools
  - static and dynamic
- DO NOT ATTACH TO YOUR LAB NETWORK!

# Binutils

## USED TO LOOK INTO BINARY FILES

- ELF format analysis with *readelf*
- object final analysis with *objdump*
- symbols and linkage with *nm*
- strings with *strings*

## EXPLOITATION FREQUENTLY DEPENDS ON BINARIES

- Not always…
  - Phishing, droppers, powershell scripts
- But frequently!
  - Exploit kits, buffer overflows, memory management bugs

Let’s get started!